IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL NO:

SPRINGFIELD, et al. Confirmation No: 1231

Serial No: 09/824,595 Group Art Unit: 2135

Filed: April 2, 2001 Examiner: Gyorfi, T.

For: METHOD AND SYSTEM FOR PROVIDING A TRUSTED FLASH BOOT SOURCE

APPEAL BRIEF

Janyce R. Mitchell
Attorney for Appellants
LENOVO Corporation
Sawyer Law Group LLP

TOPICAL INDEX

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

APPEAL NO:

SPRINGFIELD, et al. Confirmation No: 1231

Serial No: 09/824,595 Group Art Unit: 2135

Filed: April 2, 2001 Examiner: Gyorfl, T.

For: METHOD AND SYSTEM FOR PROVIDING A TRUSTED FLASH BOOT SOURCE

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Appellant herein files an Appeal Brief drafted in accordance with the provisions of 37 C.F.R. § 1.193(b)(1) as follows:

I. REAL PARTY IN INTEREST

Appellant respectfully submits that the above-captioned application is assigned, in its entirety to Lenovo Corporation of Purchase, New York.

II. RELATED APPEALS AND INTERFERENCES

Appellant states that, upon information and belief, Appellant is not aware of any co-pending appeal or interference which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12 are pending. Application Serial No. 09/824,595 (the instant application) as originally filed included claims 1-12. In response to an Office Action dated August 5, 2004, claims 1-6 were amended. Claims 1 and 6 were amended to recite that the boot source determines a source of a number of instructions initially executed as a boot source. Claims 1-5 were also amended to remove alphanumeric designation of the steps. In response to a Final Office having a mailing date of March 11, 2005, claims 1 and 6 were amended to delete the recitation added in the previous amendment. Claim 1 was also amended to harmonize claims 1 and 6, adding the limitation that the boot source determining includes writing an identity of the boot source. Claims 2-5 were amended to correct minor errors. In response to an Office Action dated November 23, 2005, claims 13-14 were added. In response to the Final Office Action dated March 27, 2006, claims 1 and 6 were amended and claims 13-14 canceled. Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12 are on appeal and all applied prospective rejections concerning claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12 are herein being appealed.

IV. STATUS OF AMENDMENT

In an Advisory Action dated June 6, 2006, the Examiner indicated that the amendments in response to the Final Office Action would be entered.

V. SUMMARY OF THE INVENTION

The present invention provides method and system for evaluating a boot source in a computer system having a processor. The method and system comprise determining the boot source used by the processor each time the computer system boots. Thus, the source of the code

used in booting the processor is determined. The determination of the boot source may include writing the identity of the boot source rather than the code actually executed, preferably in a first register. Specification, page 7, lines 1-2 (paragraph 18). For example, the location of a particular number of instructions may be written. Specification, page 6, lines 1-10 (paragraph 18). The method and system also include allowing the known boot source to be specified. The known boot source is preferably specified by writing the identity of the known boot source in a second register. Specification, page 7, lines 3-6 (paragraph 18). As a result, the boot source for the computer is determined (through the identity written) and can be verified using the known boot source. Specification, page 7, lines 6-9. Thus, the boot source can be checked to ensure that a trusted source (the known boot source) has been used. Consequently, a trusted boot source can be provided. Specification, page 7, lines 9-10.

Figure 1 depicts a conventional computer system 10. Specification, page 1, line 6. The conventional computer system 10 includes a FLASH boot source 20, which is typically coupled with the processor 12 through a bridge 16. Specification, page 1, lines 11-12. Thus, the FLASH boot source 20 is used as a boot source for the processor 12 and, once the BIOS has been loaded through booting, the computer system 10 may function. Specification, page 1, lines 12-15. However, it is possible to circumvent the FLASH boot source 20 by placing another boot source at the PCI connector 18. Specification, page 2, lines 3-6. Consequently, the conventional computer system 10 is subject to attack. The computer system 10 could be made secure by a trusted boot source—a boot source that is known and can be verified. For example, the FLASH boot source 20 could be specified as the trusted boot source and the computer system 10 could be precluded from booting from another source. Specification, page 2, lines 11-20. However, this

may adversely affect manufacturing, which typically uses a boot source other than the FLASH boot source 20. Specification, page 2, line 20-page 3, line 4.

In contrast, Figure 2 depicts one embodiment of a system 150 in accordance with the present invention for providing a trusted boot source. The system 150 is resides within the computer system 100. The computer system 100 still includes a boot source, shown as the preferred FLASH boot source, and a processor 112. Figure 2. The system 150 includes two registers 152 and 154. The register 152 is for storing the boot source of the most recent boot, while the register 154 is for storing the known boot source, the boot source from which boots are supposed to be made. Specification, page 6, lines 1-6. By checking the contents of the first register 152 against the contents of the second register 154, it can be ensured that the computer system 100 boots from a known source. Consequently, a trusted boot source can be provided. Specification, page 6, lines 10-11.

Figure 3 depicts a flow chart of one embodiment of a method 200 for providing a trusted boot source. Specification, page 6, lines 12-13. The known boot source is specified, preferably by writing the known boot source to the second register 154, via step 252. Specification, page 6, lines 16-22. In one embodiment, the identity of the FLASH boot source 140 would be written to the second register 154. The identity of the actual boot source used is determined, preferably by writing the identity of the boot source to the first register 152, via step 254. Specification, page 6, line 22-page 7, line 6. For example, as described in the specification, an "identity of the source of the first one hundred instructions" executed is written to the first register 152. Specification, page 7, lines 1-2. The first one hundred instructions themselves are not written. Instead, the identity of their *source* is stored. The identities of the boot source used and the known boot source desired to be used are, therefore, available. The identity of the boot source

used (e.g. source of code initially executed) can thus be compared to the known boot source (e.g. the FLASH boot source 140). Consequently, a trusted boot source can be provided. Specification, page 6, lines 13-16.

Figure 4 depicts one embodiment of a method 250 for providing a trusted boot source. Specification, page 7, lines 11-12. The known boot source is specified by writing the identity of the known boot source to a write-once register such as the second register 154, via step 252. Specification, page 7, lines 15-16. Each time the computer system boots, the identity of the boot source used is written to the first register 152, via step 254. Specification, page 7, lines 21-23. This identity may be the "identity of the source of the first one hundred instructions executed by the computer system 100 . . ." Specification, page 7, lines 21-22. Note that again, the actual instructions themselves are not written.

The identity of the boot source written in step 254 is checked against the known boot source in step 256. Specification, page 8, lines 2-5. Thus, it can be determined whether the boot source used was the known boot source. The computer system may then take appropriate action, via step 258. Specification, page 8, lines 6-10. The appropriate action may include acts such as shutting down if the boot source and known boot source do not match.

Thus, using the system 100 and the methods 200 and/or 250, a trusted boot source may be provided without requiring a significant change in manufacturing of the computer system 100. Specification, page 8, lines 19-21.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

(1) whether claims 1-12 are each unpatentable under 35 U.S.C. § 103 as being unpatentable over U.S. Patent No. 6,678,833 (Grawrock) in view of U.S. Patent no. 6,161,177 (Anderson).

VII. ARGUMENTS

A. Summary of the Applied Rejections

In a Final Office Action dated March 27, 2006, the Examiner rejected claims 1-14 under 35 U.S.C. § 103 as being unpatentable over Grawrock in view of Anderson. In response to Appellants' arguments previous arguments, the Examiner indicated that Anderson teaches that:

> **one can record this identity of a boot source. . . Furthermore, even if the identity of the boot source were strictly limited to the a reference to the boot source location, it is inherent to the Anderson reference that the identifying information/identity of the BIOS must include a location, as Anderson clearly teaches that the computer system involved can store multiple BIOS/boot sources . . .**

However, the Examiner further indicated that it "is unclear whether Grawrock discloses further including writing the identity of a boot source. However, Anderson discloses this limitation (col. 3, lines 20-25)."

Appellant respectfully requests that the Board reverse the Examiner's final rejection of claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12 under 35 U.S.C. § 103 and the Examiner's final rejection of claims 7 and 14 under 35 U.S.C. § 103.

B. The Cited Prior Art

Grawrock describes a system which provides a boot block *identifier* from the boot block memory unit, either the first time the computer system starts up or each time the system starts up. Grawrock, col. 3, lines 57-67. In particular, Grawrock states that the:

> boot block memory unit loads and records its boot block identifier into the memory . . . Next, the boot block memory unit locates and loads the BIOS for execution . . . The BIOS (or a representation thereof) is loaded to the TPM and a BIOS identifier is recorded . . .

Grawrock, col. 4, lines 25-30. Thus, Grawrock does state that a BIOS identifier and the boot block identifier are recorded. However, the boot block identifier is a hash of "boot information."

Grawrock, col. 3, lines 57-61. Grawrock further states that the "boot information" is basically an image or series of sub-images that collectively *represent* the boot block code. Grawrock, col. 3, lines 45-50. Thus, the boot information corresponds to the boot code itself, rather than to an identity of the boot source. In response to challenges, a digital signature is provided. Grawrock, col. 4, lines 10-16. This digital signature is a combination of the boot block identifier, keying material, certificates, and other similar information. Grawrock, col. 4, lines 17-18. Consequently, Grawrock describes providing a boot block identifier and a digital signature incorporating the boot block identifier that are both based on a representation of the boot block code actually used rather than on the identity of the boot source.

Anderson is concerned with ensuring that the central processing unit (CPU) and BIOS are compatible. Anderson, Abstract. Anderson describes a system that reads "identifying data" for the BIOS. Anderson, col. 4, lines 50-54. Anderson states that this "BIOS identifying data [is data] specifying the CPU or other chip set components corresponding to the BIOS program, i.e., the CPU that the BIOS program was designed to be executed by or the chip set components that the BIOS program was designed to operate with." Anderson, col. 3, lines 5-10. This identifying data is sufficient to determine whether the BIOS and hardware correspond to the same central processing unit and chip set. Anderson, col. 2, line 65-col. 3, line 20. Anderson also states that the BIOS identifying data corresponds to the last executed BIOS program and is compared with stored hardware data. Anderson, col. 3, lines 22-26. Thus, it can be verified whether the BIOS program executed corresponds to the hardware. Anderson, col. 3, lines 27-35. Anderson also describes performing a test upon each power up. Anderson, col. 4, line 50-col. 5, line 5. to do so, the system reads the hardware identifying data and data that relates to the BIOS. Anderson, col. 4, lines 50-54. The information that has been read to determine whether the BIOS and hardware

match. Anderson, col. 4, lines 54-60. If the information matches, no further action is taken. Anderson, col. 4, lines 60-61. If, however, the information does not indicate that the hardware and BIOS are compatible, then remedial action may be taken. Anderson, col. 4, lines 61-62.

C. Claims 1-12 Are Not Unpatentable Under 35 U.S.C. § 103.

Appellant respectfully submits that the applied rejections of claims 1 and 6 under 35 U.S.C. § 103 are without merit as the Examiner has completely failed to explain why Grawrock in view of Anderson teaches or suggests the method and system recited in claims 1 and 6. Independent claims 1 and 6 recite a method and system, respectively, for evaluating a boot source in a computer system. In particular, method recited in claim 1 includes:

> determining the boot source used by the processor each time the computer system boots, the boot source determining further including writing an identity of the boot source, the identity of the boot source including a location of a particular number of instructions initially executed; and
>
> allowing the boot source to be specified once as a known boot source.

Similarly, independent claim 6 recites a system including:

> a first register for storing an identity of the boot source used by the processor each time the computer system boots, the identity of the boot source including a location of a particular number of instructions initially executed; and
>
> a second register for allowing the boot source to be specified once as a known boot source.

Thus, claims 1 and 6 recite that *each time the computer system boots*, the identity of the boot source is determined. This identity of the boot source includes the location of a number of instructions initially executed. Thus, each time the computer system boots, the identity of the boot source (including the location of instructions initially executed) is written. Consequently, it can be determined whether the boot source is a trusted boot source. Thus, the source, or location, of the

instructions that are actually executed can be provided and independently verified. Specification, page 8, lines 13-15. Because the source of the instructions is verified, the boot source is evaluated and, therefore, trusted. As a result, a trusted boot source can be reliably provided. Specification, page 8, lines 15-16.

Grawrock in view of Anderson fails to teach or suggest writing an identity of the boot source, including writing the location of a number of instructions initially executed each time that the system boots. Grawrock does *not* describe writing the location of a number of instructions initially executed each time that the system boots. Instead, Grawrock discloses storing a "boot block identifier" for the boot source. Grawrock specifically states that this boot block identifier is a hash of "boot information." Grawrock, col. 3, lines 57-61. Grawrock further states that the "boot information may be an image of the boot block code or multiple sub-images that collectively represent the boot block code, which is used to monitor the boot process." Grawrock, col. 3, lines 45-50. Thus, the boot block identifier corresponds to the code actually booted. Stated differently, the boot block identifier of Grawrock merely corresponds to the contents of (instructions in) the boot source, not the recited identity (location of instructions executed) of the boot source. Grawrock alone, therefore, fails to teach or suggest storing of the recited boot block identity each time the computer system is booted.

Anderson fails to remedy the defects of Grawrock. Anderson describes a system that reads "identifying data" for the BIOS. Anderson, col. 4, lines 50-54. However, Anderson specifically states that this BIOS identifying data specifies the CPU or other chip set components corresponding to the BIOS program. Consequently, Anderson describes determining identifying data that merely determines whether the BIOS and hardware correspond to the same central

processing unit and chip set. This identifying data is, therefore, distinct from the location of a particular number of instructions initially executed.

Furthermore, Anderson fails to teach or suggest storing the identifying data *each time* that the computer system is booted. Although Anderson describes performing a test upon each power up, this test does not include writing the location of instructions initially executed. Instead, the hardware identifying data and data that relates to the BIOS are read and checked. Thus, Anderson further fails to teach or suggest writing the recited identity of the boot source each time the computer system is booted. Consequently, Anderson also fails to teach or suggest writing the location of a number of instructions initially executed each time that the system boots.

If the teachings of Anderson were added to those of Grawrock, then in addition to storing the boot block identifier of Grawrock, the combination might also perform the test of Anderson to determine whether the hardware and BIOS are compatible. However, neither the boot block identifier of Grawrock nor the reading of BIOS and hardware information of Anderson include the location of a particular number of instructions initially executed. Stated differently, even if the teachings of Anderson were combined with those of Grawrock, the combination would not write the identity of the boot source, including writing the location of a number of instructions initially executed, each time the computer system boots. Consequently, Grawrock in view of Anderson fail to teach or suggest the method and system recited in claims 1 and 6, respectively. Accordingly, Appellant respectfully submits that claims 1 and 6 are allowable over the cited references.

Claims 2-5 and 7-12 depend upon independent claims 1 and 6, respectively. Consequently, claims 2-5 and 7-12 are allowable for the same reasons discussed above with respect to claims 1 and 6.

Accordingly Appellant respectfully requests that the Board reverse the final rejection of claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 12 under 35 U.S.C. § 103.

D. Summary of Arguments

For all the foregoing reasons, it is respectfully submitted that Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, and 12 (all the claims presently in the application) are patentable for defining subject matter which would not have been obvious under 35 U.S.C. § 103. Thus, Appellant respectfully requests that the Board reverse the rejection of all the appealed Claims and find each of these Claims allowable.

Note: For convenience of detachment without disturbing the integrity of the remainder of pages of this Appeal Brief, Appellant's "APPENDIX" section is contained on separate sheets following the signatory portion of this Appeal Brief.

Authorization for payment of the required Brief fee is contained in the transmittal letter for this Brief. Please charge any fee that may be necessary for the continued pendency of this application to Deposit Account No. 50-3533 (Lenovo).

Very truly yours,

September 19, 2006

*/Janyce R. Mitchell/*Reg. No. 40,095
Janyce R. Mitchell
Attorney for Appellants
Reg. No. 40,095
(650) 493-4540

VIII. CLAIMS APPENDIX

1. A method for evaluating a boot source in a computer system having a processor comprising:

determining the boot source used by the processor each time the computer system boots, the boot source determining further including writing an identity of the boot source, the identity of the boot source including a location of a particular number of instructions initially executed; and

allowing the boot source to be specified once as a known boot source.

2. The method of claim 1 wherein the known boot source allowing step further includes:

specifying that the known boot source to be a FLASH boot source.

3. The method of claim 2 wherein the specifying step further includes:

writing the identity of the FLASH boot source in a write-once register which identifies the boot source for future boots.

4. The method of claim 1 wherein the determining step further includes:

writing the identity of the boot source in a register each time the computer system boots.

5. The method of claim 1 further comprising:

checking the boot source determined to ensure that the boot source is the known boot source.

6. A system for evaluating a boot source in a computer system having a processor coupled with a boot source, the system comprising:

a first register for storing an identity of the boot source used by the processor each time the computer system boots, the identity of the boot source including a location of a particular number of instructions initially executed; and

a second register for allowing the boot source to be specified once as a known boot source.

7. The system of claim 6 wherein the computer system includes a bridge coupling the processor with the boot source and wherein the first register and the second register are located in the bridge.

8. The system of claim 7 wherein the bridge is a south bridge.

9. The system of claim 6 wherein the known boot source is written only once to the second register.

10. The system of claim 9 wherein the known boot source is a FLASH boot source.

11. The system of claim 6 wherein the identity of the boot source is written to the first register each time the computer system boots.

12. The system of claim 6 wherein the processor is capable of checking the boot source stored in the first register to ensure that the boot source is the known boot source.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.

TRANSMITTAL FORM	Attorney Docket No. RPS920000016US1/2031P

In re the application of: **Randall SPRINGFIELD, et al.** Confirmation No: **1231**

Serial No: **09/824,595** Group Art Unit: **2135**

Filed: **April 2, 2001** Examiner: **Gyorfi, Thomas A.**

For: **Method and System for Providing a Trusted Flash Boot Source**

ENCLOSURES *(check all that apply)*					
☐	Amendment/Reply	☐	Assignment and Recordation Cover Sheet	☐	After Allowance Communication to Group
	☐ After Final	☐	Part B-Issue Fee Transmittal	☐	Notice of Appeal
☐	Information disclosure statement	☐	Letter to Draftsman	■	Appeal Brief
	☐ Substitute Form 1449	☐	Drawings	☐	Status Letter
	☐ Reference Copies	☐	Petition	■	Postcard
☐	Extension of Time Request *	☐	Fee Address Indication Form	☐	Other Enclosure(s) *(please identify below):*
☐	Express Abandonment	☐	Terminal Disclaimer		
☐	Certified Copy of Priority Doc	☐	Power of Attorney and Revocation of Prior Powers		
☐	Response to Incomplete Appln	☐	Change of Correspondence Address		
☐	Response to Missing Parts	*Extension of Term: Pursuant to 37 CFR 1.136, Applicant petitions the Commissioner to extend the time for response for xxxxxx month(s), from to .			
	☐ Executed Declaration by Inventor(s)				

CLAIMS					
FOR	Claims Remaining After Amendment	Highest # of Claims Previously Paid For	Extra Claims	RATE	FEE
Total Claims	0	0	0	$ 50.00	$ 0.00
Independent Claims	0	0	0	$200.00	$ 0.00
				Total Fees	$ 0.00

METHOD OF PAYMENT	
☐	Check no. _____ in the amount of $ _____ is enclosed for payment of fees.
■	Charge $ 500.00 to Deposit Account No. 50-3533 (Lenovo) for payment of Appeal Brief filing fees.
■	Charge any additional fees or credit any overpayment to Deposit Account No. 50-3533 (Lenovo)

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT	
Attorney Name	Janyce R. Mitchell, Reg. No. 40,095
Signature	*/Janyce R. Mitchell/*Reg. No. 40,095 Janyce R. Mitchell
Date	September 19, 2006

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on **09/19/2006**.

Type or printed name	Jackie Tanda
Signature	Jackie Tanda